Mordell-Weil theorem for function fields

Ajay Prajapati

Indian Institute of Science, Bengaluru

April 24, 2023

Our goal

Mordell-Weil theorem for function fields

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over a field k

Our goal

Mordell-Weil theorem for function fields

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over a field $k$and let E/K be the corresponding elliptic curve over the function field $K = k(C)$.

Our goal

Mordell-Weil theorem for function fields

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over a field $k$and let E/K be the corresponding elliptic curve over the function field $K = k(C)$.If $\mathcal{E} \longrightarrow C$ does not split, then $E(K)$ is a finitely generated group.

Overview

Overview

Motivation

Elliptic surfaces appear in many guises:

1. As elliptic curves over one-dimensional function fields, and

Motivation

Elliptic surfaces appear in many guises:

1. As elliptic curves over one-dimensional function fields, and
2. As one-parameter algebraic families of elliptic curves.

Motivation

Elliptic surfaces appear in many guises:

1. As elliptic curves over one-dimensional function fields, and
2. As one-parameter algebraic families of elliptic curves.

We will concentrate on those properties of elliptic surfaces which resemble the arithmetic properties of elliptic curves defined over number fields.

Motivation

Elliptic surfaces appear in many guises:

1. As elliptic curves over one-dimensional function fields, and
2. As one-parameter algebraic families of elliptic curves.

We will concentrate on those properties of elliptic surfaces which resemble the arithmetic properties of elliptic curves defined over number fields.

1. We will restrict attention to fields of characteristic zero. (So that $k(T)$ is a perfect field and we can apply results of AEC I-III)

Families of elliptic curves:

$$y^2 = x^3 + D \qquad \text{and} \qquad y^2 = x^3 + Dx$$

for varying D.

Families of elliptic curves:

$$y^2 = x^3 + D \qquad \text{and} \qquad y^2 = x^3 + Dx$$

for varying D.
More generally, let k be a field with $\mathrm{char}(k) \neq 2$ and $A(T), B(T) \in k(T)$. Then look at the family of elliptic curves:

$$E_T : y^2 = x^3 + A(T)x + B(T) \tag{1}$$

Families of elliptic curves:

$$y^2 = x^3 + D \qquad \text{and} \qquad y^2 = x^3 + Dx$$

for varying D.
More generally, let k be a field with $\mathrm{char}(k) \neq 2$ and $A(T), B(T) \in k(T)$. Then look at the family of elliptic curves:

$$E_T : y^2 = x^3 + A(T)x + B(T) \tag{1}$$

For $T = t$, E_t will be an elliptic curve provided

$$A(t) \neq \infty, B(t) \neq \infty, \text{ and } \Delta(t) = -16(4A(t)^3 + 27B(t)^2) \neq 0.$$

Families of elliptic curves:

$$y^2 = x^3 + D \qquad \text{and} \qquad y^2 = x^3 + Dx$$

for varying D.
More generally, let k be a field with $\mathrm{char}(k) \neq 2$ and $A(T), B(T) \in k(T)$. Then look at the family of elliptic curves:

$$E_T : y^2 = x^3 + A(T)x + B(T) \tag{1}$$

For $T = t$, E_t will be an elliptic curve provided

$$A(t) \neq \infty, B(t) \neq \infty, \text{ and } \Delta(t) = -16(4A(t)^3 + 27B(t)^2) \neq 0.$$

We can also view E_T as a single elliptic curve with discriminant

$$\Delta(T) = -16(4A(T)^3 + 27B(T)^2) \neq 0 \text{ in } k(T).$$

Example

Let $C/\mathbb{Q}$ be the (elliptic) curve

$$C : s^2 - s = t^3 - t^2;$$

Example

Let $C/\mathbb{Q}$ be the (elliptic) curve

$$C : s^2 - s = t^3 - t^2;$$

Then the equation

$$E : y^2 + (st + t - s^2)xy + s(s-1)(s-t)t^2y = x^3 + s(s-1)(s-t)tx^2$$

defines an elliptic curve E over $\mathbb{Q}(C)$ of C.

Overview

Weak Mordell-Weil Theorem [ATAEC III.2.1]

Let

$$\begin{aligned} k &\ \text{an algebraically closed field with } \mathrm{char}(k) = 0 \\ C/k &\ \text{a non-singular projective curve over } k \\ K = k(C) &\ \text{the function field of a curve } C/k \\ E/K &\ \text{an elliptic curve} \end{aligned}$$

Then the quotient group $E(K)/2E(K)$ is finite.

Weak Mordell-Weil Theorem [ATAEC III.2.1]

Let

k	an algebraically closed field with $\mathrm{char}(k) = 0$
C/k	a non-singular projective curve over k
$K = k(C)$	the function field of a curve C/k
E/K	an elliptic curve

Then the quotient group $E(K)/2E(K)$ is finite.

Proof in case of number fields

1. **Step I:** The extension field $L = K([m]^{-1}E(K))$ is an abelian extension of K, has exponent m, and is unramified outside a certain finite set of primes S.

Weak Mordell-Weil Theorem [ATAEC III.2.1]

Let

k an algebraically closed field with $\mathrm{char}(k) = 0$

C/k a non-singular projective curve over k

$K = k(C)$ the function field of a curve C/k

E/K an elliptic curve

Then the quotient group $E(K)/2E(K)$ is finite.

Proof in case of number fields

1. **Step I:** The extension field $L = K([m]^{-1}E(K))$ is an abelian extension of K, has exponent m, and is unramified outside a certain finite set of primes S.
2. **Step II:** We use Kummer theory to show that the maximal abelian extension of K of exponent m unramified outside of S is a finite extension. [VIII.1.6]

1. If $K = k(C)$ is a function field, then the "unit group" in K^* is the constant field k^*.

1. If $K = k(C)$ is a function field, then the "unit group" in K^* is the constant field k^*.
2. The "ideal class group" of a function field $K = k(C)$ is the Picard group $\mathrm{Pic}(C)$. The Picard group need not be finitely generated.

1. If $K = k(C)$ is a function field, then the "unit group" in K^* is the constant field k^*.
2. The "ideal class group" of a function field $K = k(C)$ is the Picard group $\mathrm{Pic}(C)$. The Picard group need not be finitely generated.
3. We only used the facts that the ideal class group has only finitely many elements of order m and the unit group R^* has the property that the quotient $R^*/(R^*)^m$ is finite.

1. If $K = k(C)$ is a function field, then the "unit group" in K^* is the constant field k^*.
2. The "ideal class group" of a function field $K = k(C)$ is the Picard group $\mathrm{Pic}(C)$. The Picard group need not be finitely generated.
3. We only used the facts that the ideal class group has only finitely many elements of order m and the unit group R^* has the property that the quotient $R^*/(R^*)^m$ is finite.

Proposition [ATAEC III.2.2]

Let C/k be a non-singular projective curve defined over field k. Then for any integer $m \geq 1$, the Picard group $\mathrm{Pic}(C)[m]$ is finite.

Proof Sketch

1. If L/K is a finite Galois extension and if we can prove that $E(L)/2E(L)$ is finite, then $E(K)/2E(K)$ is also finite.

Proof Sketch

1. If L/K is a finite Galois extension and if we can prove that $E(L)/2E(L)$ is finite, then $E(K)/2E(K)$ is also finite.
2. So it suffices to prove (2.1) under the assumption that $E[2] \subset E(K)$. Equivalently, E has a Weierstrass equation

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad \text{with } e_1, e_2, e_3 \in K.$$

Proof Sketch

1. If L/K is a finite Galois extension and if we can prove that $E(L)/2E(L)$ is finite, then $E(K)/2E(K)$ is also finite.
2. So it suffices to prove (2.1) under the assumption that $E[2] \subset E(K)$. Equivalently, E has a Weierstrass equation

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad \text{with } e_1, e_2, e_3 \in K.$$

Consider the map

$$\phi : E(K)/2E(K) \longrightarrow (K^*/K^{*2}) \times (K^*/K^{*2})$$

defined by

$$P = (x, y) \longrightarrow \begin{cases} (x - e_1, x - e_2) & \text{if } x \neq e_1, e_2, \\ ((e_1 - e_3)(e_1 - e_2), e_1 - e_2)) & \text{if } x = e_1, \\ (e_2 - e_1, (e_2 - e_3)(e_2 - e_1) & \text{if } x = e_2, \\ (1, 1) & \text{if } x = \infty (P = O) \end{cases}$$

In the case that K is a number field, it was proved in [AEC, X.1.4] (Complete 2-descent) that ϕ is an injective homomorphism, and the same proof works for an arbitrary field K.

In the case that K is a number field, it was proved in [AEC, X.1.4] (Complete 2-descent) that ϕ is an injective homomorphism, and the same proof works for an arbitrary field K. We prove that $\phi(E(K)/2E(K))$ is finite.

In the case that K is a number field, it was proved in [AEC, X.1.4] (Complete 2-descent) that ϕ is an injective homomorphism, and the same proof works for an arbitrary field K. We prove that $\phi(E(K)/2E(K))$ is finite.

Lemma [ATAEC III.2.3.1]

Suppose that E has a Weierstrass equation of the form

$$E : y^2 = (x - e_3)(x - e_2)(x - e_3) \quad \text{with } e_1, e_2, e_3 \in K.$$

In the case that K is a number field, it was proved in [AEC, X.1.4] (Complete 2-descent) that ϕ is an injective homomorphism, and the same proof works for an arbitrary field K. We prove that $\phi(E(K)/2E(K))$ is finite.

Lemma [ATAEC III.2.3.1]

Suppose that E has a Weierstrass equation of the form

$$E : y^2 = (x - e_3)(x - e_2)(x - e_3) \quad \text{with } e_1, e_2, e_3 \in K.$$

Let $S \subset C$ be the set of points where anyone of e_1, e_2, e_3 has a pole, together with the points where

$$\Delta = (e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$$

vanishes. Then for any point $P = (x, y) \in E(K)$ with $x \neq e_1$,

In the case that K is a number field, it was proved in [AEC, X.1.4] (Complete 2-descent) that ϕ is an injective homomorphism, and the same proof works for an arbitrary field K. We prove that $\phi(E(K)/2E(K))$ is finite.

Lemma [ATAEC III.2.3.1]

Suppose that E has a Weierstrass equation of the form

$$E : y^2 = (x - e_3)(x - e_2)(x - e_3) \quad \text{with } e_1, e_2, e_3 \in K.$$

Let $S \subset C$ be the set of points where anyone of e_1, e_2, e_3 has a pole, together with the points where

$$\Delta = (e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$$

vanishes. Then for any point $P = (x, y) \in E(K)$ with $x \neq e_1$,

$$\operatorname{ord}_t(x - e_1) \equiv 0 \pmod 2) \text{ for all } t \in C \text{ with } t \notin S.$$

Here $\operatorname{ord}_t : k(C)^* \longrightarrow \mathbb{Z}$ is the normalized valuation on $k(C)$ which measures the order of vanishing of a function at t.

Let S be as before, and define a subgroup of K^*/K^{*2} by

$$K(S,2) = \left\{ f \in K^*/K^{*2} : \mathrm{ord}_t(f) \equiv 0 (\mathrm{mod} 2) \text{ for all } t \notin S \right\}.$$

Let S be as before, and define a subgroup of K^*/K^{*2} by

$$K(S,2) = \left\{ f \in K^*/K^{*2} : \operatorname{ord}_t(f) \equiv 0 (\operatorname{mod} 2) \text{ for all } t \notin S \right\}.$$

Then we have an injective homomorphism

$$\phi : E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

Let S be as before, and define a subgroup of K^*/K^{*2} by

$$K(S,2) = \{f \in K^*/K^{*2} : \mathrm{ord}_t(f) \equiv 0 (\mathrm{mod} 2) \text{ for all } t \notin S\}.$$

Then we have an injective homomorphism

$$\phi : E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

Lemma [ATAEC III.2.3.2]

Let $S \subset C$ be a finite set of points, and let $m \geq 1$ be an integer.

Let S be as before, and define a subgroup of K^*/K^{*2} by

$$K(S,2) = \left\{ f \in K^*/K^{*2} : \mathrm{ord}_t(f) \equiv 0 (\bmod 2) \text{ for all } t \notin S \right\}.$$

Then we have an injective homomorphism

$$\phi : E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

Lemma [ATAEC III.2.3.2]

Let $S \subset C$ be a finite set of points, and let $m \geq 1$ be an integer.Then the group

$$K(S,m) = \left\{ f \in \frac{K^*}{K^{*m}} : \mathrm{ord}_t(f) \equiv 0 \bmod m \text{ for all } t \notin S \right\}$$

is a finite subgroup of K^*/K^{*m}.

Let S be as before, and define a subgroup of K^*/K^{*2} by

$$K(S,2) = \left\{ f \in K^*/K^{*2} : \mathrm{ord}_t(f) \equiv 0 (\mathrm{mod} 2) \text{ for all } t \notin S \right\}.$$

Then we have an injective homomorphism

$$\phi : E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

Lemma [ATAEC III.2.3.2]

Let $S \subset C$ be a finite set of points, and let $m \geq 1$ be an integer. Then the group

$$K(S,m) = \left\{ f \in \frac{K^*}{K^{*m}} : \mathrm{ord}_t(f) \equiv 0 \bmod m \text{ for all } t \notin S \right\}$$

is a finite subgroup of K^*/K^{*m}.

1. Reduce to the case that $S = \emptyset$.

Let S be as before, and define a subgroup of K^*/K^{*2} by

$$K(S,2) = \left\{ f \in K^*/K^{*2} : \mathrm{ord}_t(f) \equiv 0 (\mathrm{mod} 2) \text{ for all } t \notin S \right\}.$$

Then we have an injective homomorphism

$$\phi : E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

Lemma [ATAEC III.2.3.2]

Let $S \subset C$ be a finite set of points, and let $m \geq 1$ be an integer. Then the group

$$K(S,m) = \left\{ f \in \frac{K^*}{K^{*m}} : \mathrm{ord}_t(f) \equiv 0 \bmod m \text{ for all } t \notin S \right\}$$

is a finite subgroup of K^*/K^{*m}.

1. Reduce to the case that $S = \emptyset$.
2. Define a map $K(\emptyset, m) \longrightarrow \mathrm{Pic}(C)[m]$. Prove that it is injective.

Overview

Let $K = k(C)$ be the function field of a non-singular algebraic curve C/k and let E/K be an elliptic curve defined over K.

Let $K = k(C)$ be the function field of a non-singular algebraic curve C/k and let E/K be an elliptic curve defined over K.

Definition

The height of an element $f \in K$ is defined to be

$$h(f) = \deg(f : C \longrightarrow \mathbb{P}^1).$$

Let $K = k(C)$ be the function field of a non-singular algebraic curve C/k and let E/K be an elliptic curve defined over K.

Definition

The height of an element $f \in K$ is defined to be

$$h(f) = \deg(f : C \longrightarrow \mathbb{P}^1).$$

The height of a point $P \in E(K)$ is defined to be

$$h(P) = \begin{cases} 0 & \text{if } P = O, \\ h(x) & \text{if } P = (x, y). \end{cases}$$

(Descent Theorem)

Let A be an abelian group. Suppose that there exists a (height) function $h : A \longrightarrow \mathbb{R}$ with the following three properties:

(Descent Theorem)

Let A be an abelian group. Suppose that there exists a (height) function $h : A \longrightarrow \mathbb{R}$ with the following three properties:

1. Let $Q \in A$. $\exists$ constant C_1, depending on A and Q, such that

$$h(P+Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A$$

(Descent Theorem)

Let A be an abelian group. Suppose that there exists a (height) function $h : A \longrightarrow \mathbb{R}$ with the following three properties:

1. Let $Q \in A$. $\exists$ constant C_1, depending on A and Q, such that

$$h(P+Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A$$

2. $\exists$ an integer $m \geq 2$ and a constant C_2, depending on A, s.t.

$$h(mP) \geq m^2 h(P) - C_2 \quad \text{for all } P \in A.$$

(Descent Theorem)

Let A be an abelian group. Suppose that there exists a (height) function $h : A \longrightarrow \mathbb{R}$ with the following three properties:

1. Let $Q \in A$. $\exists$ constant C_1, depending on A and Q, such that
$$h(P+Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A$$
2. $\exists$ an integer $m \geq 2$ and a constant C_2, depending on A, s.t.
$$h(mP) \geq m^2 h(P) - C_2 \quad \text{for all } P \in A.$$
3. For every constant C_3, the set $\{P \in A : h(P) \leq C_3\}$ is finite.

(Descent Theorem)

Let A be an abelian group. Suppose that there exists a (height) function $h : A \longrightarrow \mathbb{R}$ with the following three properties:

1. Let $Q \in A$. $\exists$ constant C_1, depending on A and Q, such that
$$h(P+Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A$$
2. $\exists$ an integer $m \geq 2$ and a constant C_2, depending on A, s.t.
$$h(mP) \geq m^2 h(P) - C_2 \quad \text{for all } P \in A.$$
3. For every constant C_3, the set $\{P \in A : h(P) \leq C_3\}$ is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite.

(Descent Theorem)

Let A be an abelian group. Suppose that there exists a (height) function $h : A \longrightarrow \mathbb{R}$ with the following three properties:

1. Let $Q \in A$. $\exists$ constant C_1, depending on A and Q, such that
$$h(P+Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A$$
2. $\exists$ an integer $m \geq 2$ and a constant C_2, depending on A, s.t.
$$h(mP) \geq m^2 h(P) - C_2 \quad \text{for all } P \in A.$$
3. For every constant C_3, the set $\{P \in A : h(P) \leq C_3\}$ is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite. Then A is finitely generated.

Theorem [ATAEC III.3.2]

1. $h(2P) = 4h(P) + O(1)$ for all $P \in E(K)$.

Theorem [ATAEC III.3.2]

1. $h(2P) = 4h(P) + O(1)$ for all $P \in E(K)$.
2. $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1)$ for all $P, Q \in E(K)$.

Overview

Fix a non-singular projective curve C/k and take

$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in k(C)$ with $4A^3 + 27B^2 \neq 0$.

Fix a non-singular projective curve C/k and take

$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in k(C)$ with $4A^3 + 27B^2 \neq 0$.Then for almost all points $t \in C(\bar{k})$ we can evaluate A and B at t to get an elliptic curve

$$E_t : y^2 = x^3 + A(t)x + B(t).$$

Fix a non-singular projective curve C/k and take

$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in k(C)$ with $4A^3 + 27B^2 \neq 0$.Then for almost all points $t \in C(\bar{k})$ we can evaluate A and B at t to get an elliptic curve

$$E_t : y^2 = x^3 + A(t)x + B(t).$$

From another point of view, we look at the subset of $\mathbb{P}^2 \times C$ defined

$$\mathcal{E} = \{([X, Y, Z], t) \in \mathbb{P}^2 \times C : Y^2 Z = X^3 + A(t)XZ^2 + B(t)Z^3\}.$$

Fix a non-singular projective curve C/k and take

$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in k(C)$ with $4A^3 + 27B^2 \neq 0$.Then for almost all points $t \in C(\bar{k})$ we can evaluate A and B at t to get an elliptic curve

$$E_t : y^2 = x^3 + A(t)x + B(t).$$

From another point of view, we look at the subset of $\mathbb{P}^2 \times C$ defined

$$\mathcal{E} = \{([X, Y, Z], t) \in \mathbb{P}^2 \times C : Y^2 Z = X^3 + A(t)XZ^2 + B(t)Z^3\}.$$

Note that $\mathcal{E}$ is a subvariety of $\mathbb{P}^2 \times C$ of dimension two; it is a surface formed from a family of elliptic curves.

Fix a non-singular projective curve C/k and take

$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in k(C)$ with $4A^3 + 27B^2 \neq 0$.Then for almost all points $t \in C(\bar{k})$ we can evaluate A and B at t to get an elliptic curve

$$E_t : y^2 = x^3 + A(t)x + B(t).$$

From another point of view, we look at the subset of $\mathbb{P}^2 \times C$ defined

$$\mathcal{E} = \{([X, Y, Z], t) \in \mathbb{P}^2 \times C : Y^2 Z = X^3 + A(t)XZ^2 + B(t)Z^3\}.$$

Note that $\mathcal{E}$ is a subvariety of $\mathbb{P}^2 \times C$ of dimension two; it is a surface formed from a family of elliptic curves.It also comes equipped with a section

$$\sigma_0 : C \longrightarrow \mathcal{E}, \qquad t \longmapsto O_t$$

where $O_t = ([0, 1, 0], t)$.

Let C be a non-singular projective curve.

Let C be a non-singular projective curve.

Definition

An elliptic surface over C consists of the following data:

1. a surface $\mathcal{E}$, meaning a 2 dimensional projective variety,

Let C be a non-singular projective curve.

Definition

An elliptic surface over C consists of the following data:

1. a surface $\mathcal{E}$, meaning a 2 dimensional projective variety,
2. a morphism
$$\pi : \mathcal{E} \longrightarrow C$$
such that for all but finitely many points $t \in C(k)$, fiber
$$\mathcal{E}_t = \pi^{-1}(t)$$
is a non-singular curve of genus 1,

Let C be a non-singular projective curve.

Definition

An elliptic surface over C consists of the following data:

1. a surface $\mathcal{E}$, meaning a 2 dimensional projective variety,
2. a morphism
$$\pi : \mathcal{E} \longrightarrow C$$
such that for all but finitely many points $t \in C(k)$, fiber
$$\mathcal{E}_t = \pi^{-1}(t)$$
is a non-singular curve of genus 1,
3. a section to π, $\sigma_0 : C \longrightarrow \mathcal{E}$.

Let C be a non-singular projective curve.

Definition

An elliptic surface over C consists of the following data:

1. a surface $\mathcal{E}$, meaning a 2 dimensional projective variety,
2. a morphism
$$\pi : \mathcal{E} \longrightarrow C$$
such that for all but finitely many points $t \in C(k)$, fiber
$$\mathcal{E}_t = \pi^{-1}(t)$$
is a non-singular curve of genus 1,
3. a section to π, $\sigma_0 : C \longrightarrow \mathcal{E}$.

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface. The group of sections of $\mathcal{E}$ over C is denoted by $\mathcal{E}(C) = \{\text{sections } \sigma : C \longrightarrow \mathcal{E}\}$.

Definition

1. Let $\pi : \mathcal{E} \longrightarrow C$ and $\pi' : \mathcal{E}' \longrightarrow C$ be elliptic surfaces over C. A rational map from $\mathcal{E}$ to $\mathcal{E}'$ over C is a rational map $\phi : \mathcal{E} \longrightarrow \mathcal{E}'$ which commutes with the projection maps, $\pi' \circ \phi = \pi$.

Definition

1. Let $\pi : \mathcal{E} \longrightarrow C$ and $\pi' : \mathcal{E}' \longrightarrow C$ be elliptic surfaces over C. A rational map from $\mathcal{E}$ to $\mathcal{E}'$ over C is a rational map $\phi : \mathcal{E} \longrightarrow \mathcal{E}'$ which commutes with the projection maps, $\pi' \circ \phi = \pi$.
2. The elliptic surfaces $\mathcal{E}$ and $\mathcal{E}'$ are birationally equivalent over C if there is a birational isomorphism from $\mathcal{E}$ to $\mathcal{E}'$ over C.

Definition

1. Let $\pi : \mathcal{E} \longrightarrow C$ and $\pi' : \mathcal{E}' \longrightarrow C$ be elliptic surfaces over C. A rational map from $\mathcal{E}$ to $\mathcal{E}'$ over C is a rational map $\phi : \mathcal{E} \longrightarrow \mathcal{E}'$ which commutes with the projection maps, $\pi' \circ \phi = \pi$.
2. The elliptic surfaces $\mathcal{E}$ and $\mathcal{E}'$ are birationally equivalent over C if there is a birational isomorphism from $\mathcal{E}$ to $\mathcal{E}'$ over C.

We want to prove that the theory of elliptic curves over $k(C)$ is the same as the birational theory of elliptic surfaces.

Proposition [ATAEC III.3.8.]

1. Let $E/k(C)$ an elliptic curve. To each Weierstrass equn for E,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in k(C),$$

let $\mathcal{E}(A, B)$ be the associated elliptic surface.

Proposition [ATAEC III.3.8.]

1. Let $E/k(C)$ an elliptic curve. To each Weierstrass equn for E,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in k(C),$$

let $\mathcal{E}(A, B)$ be the associated elliptic surface. Then all of the $\mathcal{E}(A, B)$ associated to E are k-birationally equivalent over C.

Proposition [ATAEC III.3.8.]

1. Let $E/k(C)$ an elliptic curve. To each Weierstrass equn for E,
$$E : y^2 = x^3 + Ax + B, \quad A, B \in k(C),$$
let $\mathcal{E}(A, B)$ be the associated elliptic surface. Then all of the $\mathcal{E}(A, B)$ associated to E are k-birationally equivalent over C.
2. Let $\mathcal{E}$ be an elliptic surface over C defined over k.

Proposition [ATAEC III.3.8.]

1. Let $E/k(C)$ an elliptic curve. To each Weierstrass equn for E,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in k(C),$$

let $\mathcal{E}(A, B)$ be the associated elliptic surface.Then all of the $\mathcal{E}(A, B)$ associated to E are k-birationally equivalent over C.

2. Let $\mathcal{E}$ be an elliptic surface over C defined over k. Then $\mathcal{E}$ is k-birationally equivalent over C to $\mathcal{E}(A, B)$ for some $A, B \in k(C)$.

Proposition [ATAEC III.3.8.]

1. Let $E/k(C)$ an elliptic curve. To each Weierstrass equn for E,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in k(C),$$

let $\mathcal{E}(A, B)$ be the associated elliptic surface.Then all of the $\mathcal{E}(A, B)$ associated to E are k-birationally equivalent over C.

2. Let $\mathcal{E}$ be an elliptic surface over C defined over k. Then $\mathcal{E}$ is k-birationally equivalent over C to $\mathcal{E}(A, B)$ for some $A, B \in k(C)$. Further, the elliptic curve

$$E : y^2 = x^3 + Ax + B$$

over $k(C)$ is uniquely determined (up to $k(C)$-iso) by $\mathcal{E}$.

Proposition [ATAEC III.3.8.]

1. Let $E/k(C)$ an elliptic curve. To each Weierstrass equn for E,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in k(C),$$

let $\mathcal{E}(A, B)$ be the associated elliptic surface.Then all of the $\mathcal{E}(A, B)$ associated to E are k-birationally equivalent over C.

2. Let $\mathcal{E}$ be an elliptic surface over C defined over k. Then $\mathcal{E}$ is k-birationally equivalent over C to $\mathcal{E}(A, B)$ for some $A, B \in k(C)$. Further, the elliptic curve

$$E : y^2 = x^3 + Ax + B$$

over $k(C)$ is uniquely determined (up to $k(C)$-iso) by $\mathcal{E}$.

3. Let $E/k(C)$ be an elliptic curve and $\mathcal{E} \to C$ an elliptic surface associated to E as in (a). Then

$$k(\mathcal{E}) \cong k(C)(E) \quad \text{as } k(C)\text{-algebras.}$$

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.(We prove that $\Omega_{E/k(C)}$ is atmost 1 dimensional.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4A' = A$ and $u^6B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.(We prove that $\Omega_{E/k(C)}$ is atmost 1 dimensional.So E has genus atmost 1.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.(We prove that $\Omega_{E/k(C)}$ is atmost 1 dimensional.So E has genus atmost 1.Then derive a contradiction assuming that E has genus 0).

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.(We prove that $\Omega_{E/k(C)}$ is atmost 1 dimensional.So E has genus atmost 1.Then derive a contradiction assuming that E has genus 0).Furthermore, the section $\sigma_0 : C \longrightarrow \mathcal{E}$ corresponds to a point $P_0 \in E(k(C))$.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4A' = A$ and $u^6B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.(We prove that $\Omega_{E/k(C)}$ is atmost 1 dimensional.So E has genus atmost 1.Then derive a contradiction assuming that E has genus 0).Furthermore, the section $\sigma_0 : C \longrightarrow \mathcal{E}$ corresponds to a point $P_0 \in E(k(C))$.So E is an elliptic curve over $k(C)$.

Proof Idea:

1. Take another Weierstrass equation. Then $\exists u \in k(C)^*$ such that $u^4 A' = A$ and $u^6 B' = B$. Then construct an explicit birational equivalence $\mathcal{E}(A', B') \longrightarrow \mathcal{E}(A, B)$.
2. $\pi : \mathcal{E} \longrightarrow C$ induces an inclusion $k(C) \hookrightarrow k(\mathcal{E})$.This is of transcendence degree 1.So there exists a curve, unique upto $k(C)$-isomorphism, such that $k(C)(E) \cong k(\mathcal{E})$ as $k(C)$-algebras.
3. Prove that E has genus 1.(We prove that $\Omega_{E/k(C)}$ is atmost 1 dimensional.So E has genus atmost 1.Then derive a contradiction assuming that E has genus 0).Furthermore, the section $\sigma_0 : C \longrightarrow \mathcal{E}$ corresponds to a point $P_0 \in E(k(C))$.So E is an elliptic curve over $k(C)$.Write Weierstrass equation for $E : y^2 = x^3 + Ax + B$ with $A, B \in k(C)$. Then $\mathcal{E}$ is birationally equivalent to $\mathcal{E}(A, B)$.

Proposition

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over k.

1. Let $\sigma_1, \sigma_2 \in \mathcal{E}(C/k)$ be sections defined over k. Then the maps $\sigma_1 + \sigma_2$ and $-\sigma_2$ described above are in $\mathcal{E}(C/k)$.

Proposition

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over k.

1. Let $\sigma_1, \sigma_2 \in \mathcal{E}(C/k)$ be sections defined over k. Then the maps $\sigma_1 + \sigma_2$ and $-\sigma_2$ described above are in $\mathcal{E}(C/k)$.
2. The operations $(\sigma_1, \sigma_2) \longmapsto \sigma_1 + \sigma_2$ and $\sigma \mapsto -\sigma$ make $\mathcal{E}(C/k)$ into an abelian group.

Proposition

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over k.

1. Let $\sigma_1, \sigma_2 \in \mathcal{E}(C/k)$ be sections defined over k. Then the maps $\sigma_1 + \sigma_2$ and $-\sigma_2$ described above are in $\mathcal{E}(C/k)$.
2. The operations $(\sigma_1, \sigma_2) \longmapsto \sigma_1 + \sigma_2$ and $\sigma \mapsto -\sigma$ make $\mathcal{E}(C/k)$ into an abelian group.
3. Let $E/k(C)$ be the elliptic curve associated to $\mathcal{E}$ as described in (3.8).

Proposition

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over k.

1. Let $\sigma_1, \sigma_2 \in \mathcal{E}(C/k)$ be sections defined over k. Then the maps $\sigma_1 + \sigma_2$ and $-\sigma_2$ described above are in $\mathcal{E}(C/k)$.
2. The operations $(\sigma_1, \sigma_2) \longmapsto \sigma_1 + \sigma_2$ and $\sigma \mapsto -\sigma$ make $\mathcal{E}(C/k)$ into an abelian group.
3. Let $E/k(C)$ be the elliptic curve associated to $\mathcal{E}$ as described in (3.8).Then there is a natural group isomorphism

$$\begin{array}{rl} E(k(C)) & \xrightarrow{\sim} \mathcal{E}(C/k), \\ P = (x_P, y_P) & \longmapsto (\sigma_P : t \to ((x_P(t), y_P(t)), t)). \end{array}$$

Proof Idea

1. (1) $(\sigma_1 + \sigma_2)(t)$ and $(-\sigma)(t)$ are rational maps. Since C is a non-singular curve, they are morphisms.

Proof Idea

1. (1) $(\sigma_1 + \sigma_2)(t)$ and $(-\sigma)(t)$ are rational maps. Since C is a non-singular curve, they are morphisms.
2. (2) Associativity and commutativity holds because they hold pointwise on an open dense subset.

Proof Idea

1. (1) $(\sigma_1 + \sigma_2)(t)$ and $(-\sigma)(t)$ are rational maps. Since C is a non-singular curve, they are morphisms.
2. (2) Associativity and commutativity holds because they hold pointwise on an open dense subset.
3. (3) This is easy to see.

Overview

Want to show that sets of bounded height in $E(K)$ are necessarily finite. But this is not true in general.

Example

let E_0/k be an elliptic curve, let $\mathcal{E} = E_0 \times C$ be the elliptic surface with $\mathcal{E} \to C$ being projection onto the second factor, and let E/K be the corresponding elliptic curve over K.

Want to show that sets of bounded height in $E(K)$ are necessarily finite. But this is not true in general.

Example

let E_0/k be an elliptic curve, let $\mathcal{E} = E_0 \times C$ be the elliptic surface with $\mathcal{E} \to C$ being projection onto the second factor, and let E/K be the corresponding elliptic curve over K.Then every point $\gamma \in E_0(k)$ gives a section

$$\sigma_\gamma : C \longrightarrow \mathcal{E} = E_0 \times C, \quad t \longmapsto (\gamma, t),$$

and this section corresponds to a point $P_\gamma \in E(K)$.

Want to show that sets of bounded height in $E(K)$ are necessarily finite. But this is not true in general.

Example

let E_0/k be an elliptic curve, let $\mathcal{E} = E_0 \times C$ be the elliptic surface with $\mathcal{E} \to C$ being projection onto the second factor, and let E/K be the corresponding elliptic curve over K.Then every point $\gamma \in E_0(k)$ gives a section

$$\sigma_\gamma : C \longrightarrow \mathcal{E} = E_0 \times C, \quad t \longmapsto (\gamma, t),$$

and this section corresponds to a point $P_\gamma \in E(K)$.Clearly, distinct γ 's give distinct P_γ 's, and just as clearly the map

$$E_0(k) \longrightarrow E(K), \quad \gamma \longmapsto P_\gamma,$$

is a homomorphism.

Definition

An elliptic surface $\mathcal{E} \longrightarrow C$ splits (over k) if there is an elliptic curve E_0/k and a birational isomorphism

$$i : \mathcal{E} \xrightarrow{\sim} E_0 \times C$$

Definition

An elliptic surface $\mathcal{E} \longrightarrow C$ splits (over k) if there is an elliptic curve E_0/k and a birational isomorphism

$$i : \mathcal{E} \xrightarrow{\sim} E_0 \times C$$

such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\quad i \quad} & E_0 \times C \\ & {\scriptstyle \pi} \searrow \quad \swarrow {\scriptstyle proj_2} & \\ & C & \end{array}$$

There are several other ways of characterizing split elliptic surfaces.

Proposition [ATAEC III.5.1]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k, and let E/K be the corresponding EC over $K = k(C)$. The following are equivalent:

There are several other ways of characterizing split elliptic surfaces.

Proposition [ATAEC III.5.1]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k, and let E/K be the corresponding EC over $K = k(C)$. The following are equivalent:

1. The elliptic surface $\mathcal{E} \longrightarrow C$ splits over k.

There are several other ways of characterizing split elliptic surfaces.

Proposition [ATAEC III.5.1]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k, and let E/K be the corresponding EC over $K = k(C)$. The following are equivalent:

1. The elliptic surface $\mathcal{E} \longrightarrow C$ splits over k.
2. There is an elliptic curve E_0/k and an isomorphism $E \xrightarrow{\sim} E_0$ defined over K.

Example

Take $C = \mathbb{P}^1$ and $K = k(T)$, and consider the elliptic surfaces

$$\mathcal{E}_1 : y^2 = x^3 + 1, \quad \mathcal{E}_2 : y^2 = x^3 + T^6,$$
$$\mathcal{E}_3 : y^2 = x^3 + T, \quad \mathcal{E}_4 : y^2 = x^3 + x + T.$$

Example

Take $C = \mathbb{P}^1$ and $K = k(T)$, and consider the elliptic surfaces

$$\begin{aligned} \mathcal{E}_1 : y^2 = x^3 + 1, \quad \mathcal{E}_2 : y^2 = x^3 + T^6, \\ \mathcal{E}_3 : y^2 = x^3 + T, \quad \mathcal{E}_4 : y^2 = x^3 + x + T. \end{aligned}$$

Also let E_0/k be the elliptic curve

$$E_0 : y^2 = x^3 + 1$$

Example

Take $C = \mathbb{P}^1$ and $K = k(T)$, and consider the elliptic surfaces

$$\mathcal{E}_1 : y^2 = x^3 + 1, \quad \mathcal{E}_2 : y^2 = x^3 + T^6,$$
$$\mathcal{E}_3 : y^2 = x^3 + T, \quad \mathcal{E}_4 : y^2 = x^3 + x + T.$$

Also let E_0/k be the elliptic curve

$$E_0 : y^2 = x^3 + 1$$

Then $\mathcal{E}_1$ is clearly split over k, since it is precisely $E_0 \times C$.

Example

Take $C = \mathbb{P}^1$ and $K = k(T)$, and consider the elliptic surfaces

$$\begin{aligned} \mathcal{E}_1 : y^2 = x^3 + 1, \quad \mathcal{E}_2 : y^2 = x^3 + T^6, \\ \mathcal{E}_3 : y^2 = x^3 + T, \quad \mathcal{E}_4 : y^2 = x^3 + x + T. \end{aligned}$$

Also let E_0/k be the elliptic curve

$$E_0 : y^2 = x^3 + 1$$

Then $\mathcal{E}_1$ is clearly split over k, since it is precisely $E_0 \times C$. The surface $\mathcal{E}_2$ also splits over k, as can be seen from the isomorphism

$$\mathcal{E}_2 \xrightarrow{\sim} E_0 \times C, \quad ((x, y), t) \longmapsto \left(\left(t^{-2}x, t^{-3}y\right), t\right).$$

Example

Take $C = \mathbb{P}^1$ and $K = k(T)$, and consider the elliptic surfaces

$$\mathcal{E}_1 : y^2 = x^3 + 1, \quad \mathcal{E}_2 : y^2 = x^3 + T^6,$$
$$\mathcal{E}_3 : y^2 = x^3 + T, \quad \mathcal{E}_4 : y^2 = x^3 + x + T.$$

Also let E_0/k be the elliptic curve

$$E_0 : y^2 = x^3 + 1$$

Then $\mathcal{E}_1$ is clearly split over k, since it is precisely $E_0 \times C$. The surface $\mathcal{E}_2$ also splits over k, as can be seen from the isomorphism

$$\mathcal{E}_2 \xrightarrow{\sim} E_0 \times C, \quad ((x,y),t) \longmapsto \left(\left(t^{-2}x, t^{-3}y\right), t\right).$$

The elliptic surface $\mathcal{E}_3$ does not split over k, although it will split if we replace the base field $k(T)$ by the larger field $k(T^{1/6})$.

Example

Take $C = \mathbb{P}^1$ and $K = k(T)$, and consider the elliptic surfaces

$$\mathcal{E}_1 : y^2 = x^3 + 1, \quad \mathcal{E}_2 : y^2 = x^3 + T^6,$$
$$\mathcal{E}_3 : y^2 = x^3 + T, \quad \mathcal{E}_4 : y^2 = x^3 + x + T.$$

Also let E_0/k be the elliptic curve

$$E_0 : y^2 = x^3 + 1$$

Then $\mathcal{E}_1$ is clearly split over k, since it is precisely $E_0 \times C$. The surface $\mathcal{E}_2$ also splits over k, as can be seen from the isomorphism

$$\mathcal{E}_2 \xrightarrow{\sim} E_0 \times C, \quad ((x, y), t) \longmapsto \left(\left(t^{-2}x, t^{-3}y\right), t\right).$$

The elliptic surface $\mathcal{E}_3$ does not split over k, although it will split if we replace the base field $k(T)$ by the larger field $k(T^{1/6})$. Finally, $\mathcal{E}_4$ does not split over k.

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,let E/K be the corresponding elliptic curve over the function field $K = k(C)$,

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,let E/K be the corresponding elliptic curve over the function field $K = k(C)$,and let d be a constant.

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,let E/K be the corresponding elliptic curve over the function field $K = k(C)$,and let d be a constant.If the set

$$\{P \in E(K) : h(P) \leq d\}$$

contains infinitely many points,

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,let E/K be the corresponding elliptic curve over the function field $K = k(C)$,and let d be a constant.If the set

$$\{P \in E(K) : h(P) \leq d\}$$

contains infinitely many points,then $\mathcal{E}$ splits over k.

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,let E/K be the corresponding elliptic curve over the function field $K = k(C)$,and let d be a constant.If the set

$$\{P \in E(K) : h(P) \leq d\}$$

contains infinitely many points,then $\mathcal{E}$ splits over k.

1. **Step I:** $\mathcal{E}$ has infinitely many sections of bounded degree (i.e., $E(K)$ has infinitely many points of bounded height), then there is a one-parameter family of such sections.

Theorem [ATAEC III.5.4]

Let $\mathcal{E} \to C$ be an elliptic surface over an algebraically closed field k,let E/K be the corresponding elliptic curve over the function field $K = k(C)$,and let d be a constant.If the set

$$\{P \in E(K) : h(P) \leq d\}$$

contains infinitely many points,then $\mathcal{E}$ splits over k.

1. **Step I:** $\mathcal{E}$ has infinitely many sections of bounded degree (i.e., $E(K)$ has infinitely many points of bounded height), then there is a one-parameter family of such sections.
2. **Step II:** If there is a one-parameter family, then $\mathcal{E}$ splits

Step I

Proposition [ATAEC III.5.5]

Under the assumptions of Theorem 5.4, there is a (non-singular projective) curve Γ/k and a dominant rational map $\phi : \Gamma \times C \to \mathcal{E}$

Step I

Proposition [ATAEC III.5.5]

Under the assumptions of Theorem 5.4, there is a (non-singular projective) curve Γ/k and a dominant rational map $\phi : \Gamma \times C \to \mathcal{E}$such that the following diagram commutes:

$$\begin{array}{ccc} \Gamma \times C & \xrightarrow{\quad\phi\quad} & \mathcal{E} \\ & {\scriptstyle proj_2}\searrow \quad \swarrow{\scriptstyle \pi} & \\ & C & \end{array}$$

Proof Sketch

Fix a Weierstrass equation for E/K of the form

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in K = k(C),$$

and we define a set $E(K, d) = P \in E(K) : h(P) \leq d$. This is given to be infinite.

The first step is to parametrize the set of maps from C to $\mathbb{P}^2$. Given $D \in \mathrm{Div}(C)$, define a map

$$\begin{aligned} L(D)^3 \backslash \{0\} &\longrightarrow \mathrm{Map}(C, \mathbb{P}^2) \\ (F_0, F_1, F_2) &\longmapsto (t \mapsto [F_0(t), F_1(t), F_2(t)]) \end{aligned}$$

The first step is to parametrize the set of maps from C to $\mathbb{P}^2$. Given $D \in \mathrm{Div}(C)$, define a map

$$\begin{aligned} L(D)^3 \backslash \{0\} &\longrightarrow \mathrm{Map}(C, \mathbb{P}^2) \\ (F_0, F_1, F_2) &\longmapsto (t \mapsto [F_0(t), F_1(t), F_2(t)]) \end{aligned}$$

Let $\ell = \dim(L(D))$ then this is really a map

$$\mathbb{P}^{3\ell-1} \cong \frac{L(D)^3 \backslash \{0\}}{k^*} \longrightarrow \mathrm{Map}(C, \mathbb{P}^2)$$

The first step is to parametrize the set of maps from C to $\mathbb{P}^2$.
Given $D \in \mathrm{Div}(C)$, define a map

$$\begin{aligned} L(D)^3 \backslash \{0\} &\longrightarrow \mathrm{Map}(C, \mathbb{P}^2) \\ (F_0, F_1, F_2) &\longmapsto (t \mapsto [F_0(t), F_1(t), F_2(t)]) \end{aligned}$$

Let $\ell = \dim(L(D))$ then this is really a map

$$\mathbb{P}^{3\ell-1} \cong \frac{L(D)^3 \backslash \{0\}}{k^*} \longrightarrow \mathrm{Map}(C, \mathbb{P}^2)$$

Some of these maps $C \longrightarrow \mathbb{P}^2$ will actually correspond to elements of $E(K)$. **The next step** is to show that the maps corresponding to $E(K)$ form an algebraic subset of $\mathbb{P}^{3\ell-1}$.

The first step is to parametrize the set of maps from C to $\mathbb{P}^2$.
Given $D \in \mathrm{Div}(C)$, define a map

$$\begin{aligned} L(D)^3 \backslash \{0\} &\longrightarrow \mathrm{Map}(C, \mathbb{P}^2) \\ (F_0, F_1, F_2) &\longmapsto (t \mapsto [F_0(t), F_1(t), F_2(t)]) \end{aligned}$$

Let $\ell = \dim(L(D))$ then this is really a map

$$\mathbb{P}^{3\ell-1} \cong \frac{L(D)^3 \backslash \{0\}}{k^*} \longrightarrow \mathrm{Map}(C, \mathbb{P}^2)$$

Some of these maps $C \longrightarrow \mathbb{P}^2$ will actually correspond to elements of $E(K)$. **The next step** is to show that the maps corresponding to $E(K)$ form an algebraic subset of $\mathbb{P}^{3\ell-1}$.
We will assume henceforth that $D \geq 0$, and we fix a basis $f_1, \ldots, f_\ell$ for $L(D)$.

The first step is to parametrize the set of maps from C to $\mathbb{P}^2$.
Given $D \in \mathrm{Div}(C)$, define a map

$$\begin{aligned} L(D)^3\backslash\{0\} &\longrightarrow \mathrm{Map}(C, \mathbb{P}^2) \\ (F_0, F_1, F_2) &\longmapsto (t \mapsto [F_0(t), F_1(t), F_2(t)]) \end{aligned}$$

Let $\ell = \dim(L(D))$ then this is really a map

$$\mathbb{P}^{3\ell-1} \cong \frac{L(D)^3\backslash\{0\}}{k^*} \longrightarrow \mathrm{Map}(C, \mathbb{P}^2)$$

Some of these maps $C \longrightarrow \mathbb{P}^2$ will actually correspond to elements of $E(K)$. **The next step** is to show that the maps corresponding to $E(K)$ form an algebraic subset of $\mathbb{P}^{3\ell-1}$.
We will assume henceforth that $D \geq 0$, and we fix a basis $f_1, \ldots, f_\ell$ for $L(D)$.Further, we choose a divisor $D' \geq 3D$ large enough so that $1, A, B \in L(D' - 3D)$, and let $h_1, \ldots, h_r$ be a basis for $L(D')$.

The first step is to parametrize the set of maps from C to $\mathbb{P}^2$.
Given $D \in \mathrm{Div}(C)$, define a map

$$\begin{aligned} L(D)^3 \backslash \{0\} &\longrightarrow \mathrm{Map}(C, \mathbb{P}^2) \\ (F_0, F_1, F_2) &\longmapsto (t \mapsto [F_0(t), F_1(t), F_2(t)]) \end{aligned}$$

Let $\ell = \dim(L(D))$ then this is really a map

$$\mathbb{P}^{3\ell-1} \cong \frac{L(D)^3 \backslash \{0\}}{k^*} \longrightarrow \mathrm{Map}(C, \mathbb{P}^2)$$

Some of these maps $C \longrightarrow \mathbb{P}^2$ will actually correspond to elements of $E(K)$. **The next step** is to show that the maps corresponding to $E(K)$ form an algebraic subset of $\mathbb{P}^{3\ell-1}$.
We will assume henceforth that $D \geq 0$, and we fix a basis $f_1, \dots, f_\ell$ for $L(D)$.Further, we choose a divisor $D' \geq 3D$ large enough so that $1, A, B \in L(D' - 3D)$, and let $h_1, \dots, h_r$ be a basis for $L(D')$.
Every element in $L(D)^3$ can be written uniquely in the form

$$F = (F_a, F_b, F_c) = (\sum_{i=1}^{\ell} a_i f_i, \sum_{i=1}^{\ell} b_i f_i, \sum_{i=1}^{\ell} c_i f_i).$$

Such an F will give an element of $E(K)$ if and only if F_a, F_b, F_c satisfy the homogeneous equation of E,

$$F_b^2 F_c = F_a^3 + AF_aF_c^2 + BF_c^3.$$

Such an F will give an element of $E(K)$ if and only if F_a, F_b, F_c satisfy the homogeneous equation of E,

$$F_b^2 F_c = F_a^3 + AF_aF_c^2 + BF_c^3.$$

In other words, F will give an element of $E(K)$ if

$$(\sum b_i f_i)^2(\sum c_i f_i) = (\sum a_i f_i)^3 + A(\sum a_i f_i)(\sum c_i f_i)^2 + B(\sum c_i f_i)^3$$

Such an F will give an element of $E(K)$ if and only if F_a, F_b, F_c satisfy the homogeneous equation of E,

$$F_b^2 F_c = F_a^3 + AF_aF_c^2 + BF_c^3.$$

In other words, F will give an element of $E(K)$ if

$$(\sum b_i f_i)^2(\sum c_i f_i) = (\sum a_i f_i)^3 + A(\sum a_i f_i)(\sum c_i f_i)^2 + B(\sum c_i f_i)^3$$

We can write this as

$$\sum_{i=1}^{r} \Phi_i(\mathbf{a}, \mathbf{b}, \mathbf{c}) h_i = 0$$

where each Φ_i is a homogeneous polynomial in the coordinates

$$[\mathbf{a}, \mathbf{b}, \mathbf{c}] = [a_1, \ldots, a_\ell, b_1, \ldots, b_\ell, c_1, \ldots, c_\ell] \in \mathbb{P}^{3\ell-1}.$$

Such an F will give an element of $E(K)$ if and only if F_a, F_b, F_c satisfy the homogeneous equation of E,

$$F_b^2 F_c = F_a^3 + AF_aF_c^2 + BF_c^3.$$

In other words, F will give an element of $E(K)$ if

$$(\sum b_i f_i)^2(\sum c_i f_i) = (\sum a_i f_i)^3 + A(\sum a_i f_i)(\sum c_i f_i)^2 + B(\sum c_i f_i)^3$$

We can write this as

$$\sum_{i=1}^{r} \Phi_i(\mathbf{a}, \mathbf{b}, \mathbf{c}) h_i = 0$$

where each Φ_i is a homogeneous polynomial in the coordinates

$$[\mathbf{a}, \mathbf{b}, \mathbf{c}] = [a_1, \ldots, a_\ell, b_1, \ldots, b_\ell, c_1, \ldots, c_\ell] \in \mathbb{P}^{3\ell-1}.$$

Now the maps $C \to \mathbb{P}^2$ from above which correspond to elements of $E(K)$ are associated to the points of the variety

$$V_D := \left\{ [\mathbf{a}, \mathbf{b}, \mathbf{c}] \in \mathbb{P}^{3\ell(D)-1} : \Phi_i(\mathbf{a}, \mathbf{b}, \mathbf{c}) = 0 \text{ for all } 1 \le i \le r \right\}$$

Lemma [ATAEC III.5.5.2]

Let g be the genus of the curve C.

Lemma [ATAEC III.5.5.2]

Let g be the genus of the curve C.If

$$\deg D \geq g + \frac{5}{2}d + \frac{1}{2}(\deg A + \deg B)$$

Lemma [ATAEC III.5.5.2]

Let g be the genus of the curve C.If

$$\deg D \geq g + \frac{5}{2}d + \frac{1}{2}(\deg A + \deg B)$$

then the image of V_D in $E(K)$ contains $E(K,d)$.

Proof

1. Let $P = (x_P, y_P) \in E(K,d)$, so, by definition, $\deg(x_P) = h(P) \leq d$.

Lemma [ATAEC III.5.5.2]

Let g be the genus of the curve C.If

$$\deg D \geq g + \frac{5}{2}d + \frac{1}{2}(\deg A + \deg B)$$

then the image of V_D in $E(K)$ contains $E(K, d)$.

Proof

1. Let $P = (x_P, y_P) \in E(K, d)$, so, by definition, $\deg(x_P) = h(P) \leq d$. Then Weierstrass equations gives us that

$$\deg(y_P) \leq \frac{3}{2}d + \frac{1}{2}(\deg(A) + \deg(B))$$

Lemma [ATAEC III.5.5.2]

Let g be the genus of the curve C.If

$$\deg D \geq g + \frac{5}{2}d + \frac{1}{2}(\deg A + \deg B)$$

then the image of V_D in $E(K)$ contains $E(K, d)$.

Proof

1. Let $P = (x_P, y_P) \in E(K, d)$, so, by definition, $\deg(x_P) = h(P) \leq d$. Then Weierstrass equations gives us that

$$\deg(y_P) \leq \frac{3}{2}d + \frac{1}{2}(\deg(A) + \deg(B))$$

2. Apply Riemann-Roch theorem to

$$D'' = D - \mathrm{div}_\infty(x_P) - \mathrm{div}_\infty(y_P)$$

Proof continued

1. Fix a divisor $D \in \mathrm{Div}(C)$ of large enough degree so that image of V_D in $E(K)$ is infinite.

Proof continued

1. Fix a divisor $D \in \mathrm{Div}(C)$ of large enough degree so that image of V_D in $E(K)$ is infinite.
2. Consider the associated elliptic surface $\mathcal{E} \longrightarrow C$. We have assigned to each point $\gamma \in V_D$ a point $P_\gamma \in E(K)$, and this corresponds to a section $\sigma_\gamma : C \longrightarrow \mathcal{E}$.

Proof continued

1. Fix a divisor $D \in \mathrm{Div}(C)$ of large enough degree so that image of V_D in $E(K)$ is infinite.
2. Consider the associated elliptic surface $\mathcal{E} \longrightarrow C$. We have assigned to each point $\gamma \in V_D$ a point $P_\gamma \in E(K)$, and this corresponds to a section $\sigma_\gamma : C \longrightarrow \mathcal{E}$. So we have a rational map

$$\phi : V_D \times C \longrightarrow \mathcal{E}, \qquad (\gamma, t) \longmapsto \sigma_\gamma(t).$$

Proof continued

1. Fix a divisor $D \in \mathrm{Div}(C)$ of large enough degree so that image of V_D in $E(K)$ is infinite.
2. Consider the associated elliptic surface $\mathcal{E} \longrightarrow C$. We have assigned to each point $\gamma \in V_D$ a point $P_\gamma \in E(K)$, and this corresponds to a section $\sigma_\gamma : C \longrightarrow \mathcal{E}$. So we have a rational map
$$\phi : V_D \times C \longrightarrow \mathcal{E}, \qquad (\gamma, t) \longmapsto \sigma_\gamma(t).$$
3. If there exists an irreducible curve $\Gamma \subset V_D$ such that the map
$$\phi : \Gamma \times C \longrightarrow \mathcal{E}, \quad (\gamma, t) \longmapsto \sigma_\gamma(t)$$
is dominant, then the proof of Proposition 5.5 will be complete.

Proof continued

1. Fix a divisor $D \in \mathrm{Div}(C)$ of large enough degree so that image of V_D in $E(K)$ is infinite.
2. Consider the associated elliptic surface $\mathcal{E} \longrightarrow C$. We have assigned to each point $\gamma \in V_D$ a point $P_\gamma \in E(K)$, and this corresponds to a section $\sigma_\gamma : C \longrightarrow \mathcal{E}$. So we have a rational map
$$\phi : V_D \times C \longrightarrow \mathcal{E}, \qquad (\gamma, t) \longmapsto \sigma_\gamma(t).$$
3. If there exists an irreducible curve $\Gamma \subset V_D$ such that the map
$$\phi : \Gamma \times C \longrightarrow \mathcal{E}, \quad (\gamma, t) \longmapsto \sigma_\gamma(t)$$
is dominant, then the proof of Proposition 5.5 will be complete. So we assume that $\phi : \Gamma \times C \to \mathcal{E}$ is not dominant for every irreducible curve $\Gamma \subset V_D$ and derive a contradiction.

Proof continued

1. Fix a divisor $D \in \mathrm{Div}(C)$ of large enough degree so that image of V_D in $E(K)$ is infinite.
2. Consider the associated elliptic surface $\mathcal{E} \longrightarrow C$. We have assigned to each point $\gamma \in V_D$ a point $P_\gamma \in E(K)$, and this corresponds to a section $\sigma_\gamma : C \longrightarrow \mathcal{E}$. So we have a rational map
$$\phi : V_D \times C \longrightarrow \mathcal{E}, \qquad (\gamma, t) \longmapsto \sigma_\gamma(t).$$
3. If there exists an irreducible curve $\Gamma \subset V_D$ such that the map
$$\phi : \Gamma \times C \longrightarrow \mathcal{E}, \quad (\gamma, t) \longmapsto \sigma_\gamma(t)$$
is dominant, then the proof of Proposition 5.5 will be complete. So we assume that $\phi : \Gamma \times C \to \mathcal{E}$ is not dominant for every irreducible curve $\Gamma \subset V_D$ and derive a contradiction.
4. Replacing Γ with a non-singular model for Γ (see Hartshorne [1, 1.6.11]) completes the proof.

Proposition [ATAEC III.5.6]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k,

Proposition [ATAEC III.5.6]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k, let Γ/k be a non-singular projective curve,

Proposition [ATAEC III.5.6]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k, let Γ/k be a non-singular projective curve, and suppose that there exists a dominant rational map $\phi : \Gamma \times C \to \mathcal{E}$ such that the following diagram commutes:

$$\begin{array}{ccc} \Gamma \times C & \xrightarrow{\quad\phi\quad} & \mathcal{E} \\ & {\scriptstyle proj_2}\searrow \quad \swarrow{\scriptstyle \pi} & \\ & C & \end{array}$$

Proposition [ATAEC III.5.6]

Let $\pi : \mathcal{E} \to C$ be an elliptic surface over k, let Γ/k be a non-singular projective curve, and suppose that there exists a dominant rational map $\phi : \Gamma \times C \to \mathcal{E}$ such that the following diagram commutes:

$$\begin{array}{ccc} \Gamma \times C & \xrightarrow{\ \phi\ } & \mathcal{E} \\ & {\scriptstyle proj_2} \searrow \quad \swarrow {\scriptstyle \pi} & \\ & C & \end{array}$$

Then $\mathcal{E}$ splits.

Overview

Mordell-Weil theorem for function fields

Let $\mathcal{E} \longrightarrow C$ be an elliptic surface defined over a field k and let E/K be the corresponding elliptic curve over the function field $K = k(C)$. If $\mathcal{E} \longrightarrow C$ does not split, then $E(K)$ is a finitely generated group.